AMENDMENTS TO THE CLAIMS

Please replace all previous versions and listings of the claims with the following listing of claims.

Listing of Claims:

1. (canceled)
2. (canceled)
3. (canceled)
4. (canceled)
5. (canceled)
6. (canceled)
7. (canceled)
8. (canceled)
9. (canceled)
10. (canceled)
11. (canceled)
12. (canceled)
13. (currently amended) A method of ~~initializing~~ populating a portion of a seed pool ~~for generating a cryptographic key for~~ with a signature value so as to allow a bypass of a cryptographic security subsystem of a processor-based device for a period of time, the method comprising the acts of:

a) prior to enabling the cryptographic security subsystem, writing a plurality of bits of data to a seed pool, the plurality of bits of data having a signature value thus allowing the bypass of the cryptographic security subsystem;

b) detecting occurrence of a first type of triggering event;

c) writing one or more bits of data to the seed pool upon termination of the first type of triggering event, the one or more bits of data altering the signature value of the seed pool.

d) enabling the cryptographic security subsystem when more than a threshold portion of the signature value of the seed pool has been altered thus terminating the bypass of the cryptographic security subsystem; and

e) generating a pseudo-random number from the seed pool, wherein the pseudo-random number is used to generate the cryptographic key for the cryptographic security subsystem of the ~~processor based~~ processor-based device.

14. (original) The method as recited in claim 13, wherein the first type of triggering event comprises a cycle of power applied to the processor-based device.

15. (original) The method as recited in claim 13, wherein the first type of triggering event is a reboot of the processor-based device.

16. (original) The method as recited in claim 13, wherein act (c) comprises the act of masking the one or more bits of data into the seed pool.

17. (original) The method as recited in claim 13, where act (c) comprises the act of capturing the one of more bits of data from a free-running timer.

18. (original) The method as recited in claim 13, comprising the acts of:

detecting a second type of triggering event;

determining if the seed pool is full; and

writing one or more bits of data to the seed pool upon termination of the second type of triggering event if the seed pool is not full.

19. (canceled)

20. (canceled)

21. (canceled)

22. (canceled)

23. (canceled)

24. (canceled)

25. (canceled)

26. (canceled)

27. (currently amended) A processor-based device comprising:

a host processing system, the host processing system comprising a processor;

a communication management system in communication with the host processing system; and

a memory system in communication with the host processing system and the communications management system,

wherein the communications management system comprises:

an interface controller;

a non-volatile memory device to store a seed pool comprising a plurality of data bits; and

security logic in communication with the interface controller and the non-volatile memory device, the security logic configured to establish a secure communication session between the processor-based device and an external device in communication with the processor-based device via the interface controller, and wherein the security logic is configured to:

write one or more bits to the seed pool, wherein the one or more bits originate from a source external to the seed pool and alter a signature value;

determine whether the plurality of data bits in the seed pool has at least a portion of the signature value; and

disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value, thus bypassing the cryptographic security subsystem and allowing access to the processor-based device for a period of time.

28. (canceled)

29. (previously presented) The processor-based device as recited in claim 27, comprising a main power supply to supply power to the processor-based device, and wherein the first type of triggering event comprises a cycle of the power supplied by the main power supply.

30. (original) The processor-based device as recited in claim 27, wherein the security logic is configured to:

    detect a second type of triggering event;

    determine whether the seed pool is fully populated; and

    write one or more data bits to the seed pool upon termination of the second type of triggering event if the seed pool is not fully populated.

31. (original) The processor-based device as recited in claim 30, wherein the second type of triggering event comprises receipt of a communication from the external device via the interface controller.

32. (original) The processor-based device as recited in claim 31, wherein the interface controller comprises a network interface controller.

33. (canceled)

34. (canceled)

35. (previously presented) The processor-based device as recited in claim 27, wherein the security logic is configured to detect a first type of triggering event, and to write one or more bits to the seed pool upon termination of the first type of triggering event.

36. (canceled)

37. (canceled)

38. (canceled)

39. (canceled)

40. (canceled)

41. (previously presented) A method of manufacturing a processor-based device comprising:

providing a memory comprising a seed pool, wherein the seed pool contains a plurality of bits having a signature value;

writing one or more bits of data to the seed pool upon termination of a first type of triggering event, the one or more bits altering the signature value; and

enabling a cryptographic security subsystem when more than a threshold amount of the signature value of the seed pool has been altered.